CONFIDENTIAL

ALL4 LOGISTICS
Road Air Sea Rail

# INFORMATION SECURITY POLICY

All4 Logistics Ltd | 57 Lakes Industrial Est. Lower Chapel Hill Braintree CM7 3RU
+44 (0) 345 351 2884 - operations@all4logistics.co.uk

| | |
|---|---|
| **Policy title:** | **Information Security Policy** |

| | | | |
|---|---|---|---|
| **Issue date:** | 10/01/2021 | **Review date:** | 10/07/2021 |

| | | | |
|---|---|---|---|
| **Version:** | v1.0 | **Issued by:** | Caroline Millea Downing - Director |

| | |
|---|---|
| **Scope:** | **ALL 4 LOGISTICS LTD**.– Entire company |

| | |
|---|---|
| **Associated documentation:** | n/a |
| **Appendices:** | n/a |
| **Approved by:** | Caroline Millea Downing - Director |
| | |

| | |
|---|---|
| **Review and consultation process:** | Regular review on date above by Caroline Millea Downing |
| **Responsibility for Implementation & Training:** | Day to day responsibility for implementation is Caroline Millea Downing<br>Day to day responsibility for training is Caroline Millea Downing |

| **Revisions:** | | |
|---|---|---|
| **Date:** | **Author:** | **Description:** |
| 10.01.2021 | Caroline Millea Downing | v1.0 Initial document |
| | | |
| | | |
| | | |

| | |
|---|---|
| **Distribution** | Digital copy on Google Drive. Paper copy stored in Head office. |

## Table of Contents

# 1. Introduction & Purpose

Information is a vitally important **ALL 4 LOGISTICS LTD** asset, and we all have a responsibility to make sure that this information is kept safe and used appropriately. Without due care, personal, research or company information can be misplaced or leaked, which is a big enough problem in itself without the added difficulty of having to protect it against increasingly proactive and sophisticated attempts at theft.

Therefore, **ALL 4 LOGISTICS LTD** has adopted an **Information Security Policy** that complies with stringent legal requirements and provides the necessary assurance that data held and processed by the **ALL 4 LOGISTICS LTD** is treated with the highest appropriate standards to keep it safe.

This information security policy is a key component of **ALL 4 LOGISTICS LTD**'s overall business management framework and provides a framework for more detailed information security documentation including system level security policies, security guidance and protocols or procedures.

This Policy is based on the following standards, regulation and legislation:

- General Data Protection Regulation (GDPR) and ICO Guidance
- Data Protection Act 2018
- Regulation of Investigatory Powers Act 2000
- ISO 9001
- Cyber Essentials Scheme

# 2. Policy aim

The aim of this policy is to set out the rules governing the secure management of our information assets by ensuring that all members of the team:

- Are aware of and fully comply with the relevant legislation as described in this policy.
- Creating and maintaining within the organisation a level of awareness of the need for information security as an integral part of the day-to-day business.
- And protecting information assets under the control of the organisation.

# 3. Scope

This policy applies to all information, information systems, networks, applications, locations, and users of **ALL 4 LOGISTICS LTD** or supplied under contract to it as well as any hardware such as laptops, mobile devices, tablets and more.

## 4. Responsibilities

- Ultimate responsibility for information security rests with the DIRECTORS of **ALL 4 LOGISTICS LTD**. They shall be responsible for managing and implementing the policy and related procedures. The directly appointed DIRECTOR as hereby mention is CAROLINE MILLEA DOWNING.

- The Managing Staff is responsible for ensuring that their permanent and temporary team members and contractors are aware of:
    - The information security policies applicable in their work areas
    - Their individual responsibilities for information security
    - How to access advice on information security matters

- All staff, team members and contractors shall comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action, including dismissal.
- Staff shall be individually responsible for the security of their physical environments where information is processed or stored.

- Each member of the team shall be responsible for the operational security of the information systems they use.

- Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use are maintained to the highest standard.

- Contracts with external parties that allow access to the organisation's information systems shall be in operation before access is allowed. These contracts shall ensure that the team members or sub-contractors of the external organisation shall comply with all appropriate security policies.

## 5. Legislation

**ALL 4 LOGISTICS LTD** is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of **ALL 4 LOGISTICS LTD** who may be held personally accountable for any breaches of information security for which they may be held responsible. **ALL 4 LOGISTICS LTD** shall comply with the following legislation and other legislation as appropriate:

- The Health and Safety at Work Act (1974)
- Data Protection Act 2018 (DPA 2018), the UK General Data Protection Regulation (UK GDPR).
- European Union Network and Information Systems (NIS) Directive.
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)

- Human Rights Act (1998)
- Regulation of Investigatory Powers Act (2000)
- Freedom of Information Act (2000)
- The Data Protection (Processing of Sensitive Personal Data) Order (2000)
- Privacy and Electronic Communications Regulations 2003

The DIRECTOR is responsible for staying up to date with existing laws and legislation that apply to **ALL 4 LOGISTICS LTD** as well as new laws and regulations that may apply to **ALL 4 LOGISTICS LTD**. The DIRECTOR is also responsible for communicating it to team members and other stakeholders.

# 6. Policy Framework

## 6.1 Definitions

**Agent**, for the purpose of this Policy, is defined as any third-party that has been contracted by the company to provide a set of services and who stores, processes or transmits company owned Data as part of those services.

**Information System** is defined as any electronic system that stores, processes, or transmits information.

**Company Data** is defined as any data that is owned or licensed by the company.

## 6.2 Personnel Security

### 6.2.1 Contracts of Employment

- Team members security requirements shall be addressed at the recruitment stage, and all contracts of employment shall contain a confidentiality clause.
- Information security expectations of team members shall be included within appropriate job definitions.
- All access rights shall be removed immediately on termination of the contract.
- All associated accounts shall be deleted or disabled on termination of the contract.
- All company assets must be returned immediately upon termination of the contract.

### 6.2.2 Intellectual Property Rights

- The organisation shall ensure that all software, applications, and operating systems are properly licensed in accordance with the publisher's recommendations.

### 6.3 Asset Management

Company devices include any computer, laptop, tablet, or mobile phone that can access company data or has been provided by the company. These devices meet the following criteria:

- All obsolete or not used software must be deleted or disabled.
- Have anti-malware installed.
- Not be jailbroken.
- Only have apps installed from their official application store.

## 7. Access Management

- Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

- Access to information shall be restricted to authorised users who have a bona-fide business need to access the information. Team members who are authorized to access information systems or restricted Data shall adhere to the appropriate Roles and Responsibilities assigned to them.

- Team members can only access laptops, computers and servers including applications they contain, by entering a unique username and password.

- Team members must make sure there are no unnecessary programs running on their devices.

- Team members shall only have admin privileges if they have a bona-fine case and for an expressly established period of time or project timeline The DIRECTOR shall have final review on whether someone should be granted administrator privileges.

- Administrator accounts shall not be used for accessing emails or for web browsing.

- Administrator accounts shall be regularly reviewed by the DIRECTOR to assess if the individuals still have a business need for privileged access.

- All administrator accounts shall enable two-factor authentication for access to all admin accounts on all accounts, applications, and machines.

- The boundary between the business systems and the Internet or other non-trusted networks shall be protected by a firewall, which shall be configured to meet the threat landscape and be regularly monitored.

- All administrative accounts must have a strong password. To achieve a strong password, the following checks must be met:
    - Between nine and twelve characters in length

  - At least one capitalised letter
  - At least one number
  - At least one special character (! @£$%&*) when allowed.

- All user and administrator accounts should have their default passwords changed to a strong password.

- All members of the team must change their passwords at least every two months and when there has been a public security breach alert.

- Admin passwords must be changed whenever there are changes in staffing.

- All administrative passwords are changed by the DIRECTOR.

- When a team member changes a password, he/she must inform the Director who confirms it has been changed via email.

- All network devices (routers, switches) are to be checked every two months for updates and security changes. User devices (desktops, laptops, mobile phones, tablets) are to be checked periodically, or at least every two months, for updates and security reviews according to each device protocol and every time there is a public security breach or a supplier/provider has informed of a security breach.

## 8. Security and Confidentiality of Users Accounts

Users assume personal responsibility for the use made of their computer, tablets and mobile devices and user accounts. This responsibility begins with selecting a secure password as per our policy and guidelines and involves maintaining the confidentiality of that password and changing the password regularly in order to assure the continued security of the accounts. For guidance in selecting a secure password, see Guidelines for Password Management. If a user believes that someone has made unauthorized use of their account, the account password should be changed immediately, and a report of the incident has to be made to the Director at caroline@all4logistics.co.uk.

## 9. Improper/Illegal Communications

Any communications that would be improper or illegal on any other medium are equally so on the computer: libellous material, obscene messages, harassment, forgery, threats, etc.

## 10. Privacy

Team members must presume that the contents of any other users' directory are private unless expressly designated otherwise, just as one would presume that the contents of someone's apartment or office are private. The only exceptions to this rule are: that in some environments, files such as "operation files" may be considered public even if the user has not expressly designated them as such; and that some services such as web pages may be considered to be

public, but only for those areas not protected by password and which are “obviously” public. An unprotected account or shared device (such as a shared disk on a networked computer) are not considered to be public unless the name or service expressly indicates that it is. In such cases, any files or other data which would appear to be private in nature, by virtue of the file name or data stored, even if “publicly accessible” should be considered to be private. The user accessing such files has a responsibility to ask the owner of the files or service if the files are intended to be publicly accessible before the user does more than a “cursory glance” sufficient to cause the question.

A user can explicitly grant access to his or her directories, files or to services run from his or her systems. However, users who issue general or vague invitations to browse through their files incur a special obligation to protect any material that they do not wish others to see. Indeed, all users are urged to maintain protection levels on their files consistent with the access each team member has been assigned to.

## 11. Protecting Confidential Information

Team members who maintain confidential information, such as records relating to employees, contractors, subcontractor, providers, suppliers or clients, are responsible for following privacy-related policies, laws, and data use agreements.

## 12. Enforcement

Violations of this Policy may result in suspension or loss of the violator's use privileges, with respect to company owned Information Systems. Additional administrative sanctions may apply up to and including termination of employment or contractor status with the company. Civil, criminal, and equitable remedies may apply.

## 9. Exceptions

Exceptions to this Policy must be approved by the Directors Board and formally documented. Policy exceptions will be reviewed on a periodic basis for appropriateness.

## 10. Cyber Essentials

We use QMS International Ltd to obtain and maintain our annual Cyber Essentials certification. It is important to **ALL 4 LOGISTICS LTD** that controls to maintain the standard are implemented and reviewed on a regular basis.

## 9. Further Information

Further information and advice on this policy can be obtained from the DIRECTOR, Caroline Millea Downing, caroline@all4logistics.co.uk, +44 (0) 345 351 2884.

Comments and suggestions to improve security are always welcome.

**Signed by**
Caroline Millea Downing
DIRECTOR

Signature:  Date: 10/01/2021

**Agreed by**
Ron Prince
Board member - Director

Signature:  Date: 10/01/2021